REMARKS

In the Office Action, the Examiner rejected claims 1-32. Claims 1, 19, 26, 27 and 29 have been amended, and claims 2, 21 and 28 have been canceled. Claims 1, 3-20, 22-27 and 29-32 remain pending. In view of the following remarks, Applicants respectfully request reconsideration and allowance of all pending claims.

Claim Rejections under 35 U.S.C. § 112, Second Paragraph

The Examiner rejected claim 26 under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the applicants regard as the invention. Claim 26 has been amended to provide the proper antecedent basis. Specifically, claim 26 now depends from claim 20 which provides "a second type of triggering event," thus addressing the issue raised by the Examiner. For this reason, Applicants respectfully request withdrawal of the rejection of claim 26 under Section 112, second paragraph.

Rejections under 35 U.S.C. § 102

The Examiner rejected claims 1-7, 12, 19-24, and 26 under 35 U.S.C. § 102(b) as being anticipated by Bruce Schneier's "Applied Cryptography", (hereinafter referred to as "Schneier"); and claims 13-18, 25 and 27-32 under 35 U.S.C. § 102(b) as being anticipated by Utz et al., (U.S. Patent No. 5,680,131, hereinafter referred to as the "Utz reference." Applicants respectfully traverse these rejections.

Legal Precedent

Anticipation under Section 102 can be found only if a single reference shows exactly what is claimed. *Titanium Metals Corp. v. Banner*, 778 F.2d 775, 227 U.S.P.Q. 773 (Fed. Cir. 1985). For a prior art reference to anticipate under Section 102, every element of the claimed invention must be identically shown in a single reference. *In re Bond*, 910 F.2d 831, 15 U.S.P.Q.2d 1566 (Fed. Cir. 1990). To maintain a proper rejection under Section 102, a single reference must teach each and every limitation of the rejected claim. *Atlas Powder v. E.I. du Pont*, 750 F.2d 1569 (Fed. Cir. 1984). The prior art reference also must show the *identical* invention *"in as complete detail as contained in the ... claim"* to support a *prima facie* case of anticipation. *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 U.S.P.Q. 2d 1913, 1920 (Fed. Cir. 1989) (emphasis added). Accordingly, Applicants need only point to a single element not found in the cited reference to demonstrate that the cited reference fails to anticipate the claimed subject matter.

Claim 1-7, 12 and 19-26

Applicants respectfully assert that Schneier does not anticipate independent claims 1 and 19 under Section 102 because not every element of the claimed invention is disclosed. Specifically, claim 1 as amended recites a method of "capturing one or more bits of data from a free-running timer." Claim 19 as amended recites security logic configured to "capture one or more bits of data from the free-running timer."

In contrast, Schneier discloses taking bits or bit streams from events, commands, or functions to create a random pool of bits. For example, Schneier lists copying keystrokes, mouse commands, and actual mouse position, among other things, to generate random numbers. Schneier, pg 426, lines 6-23. Additionally, Schneier suggests comparing the crystal oscillators from the CPU and time-of-day clocks by reading the time of day in a tight loop. Schneier, pg 426, lines 30-32. On some systems this will reflect randomness in phase jitter between the two oscillators. Schneier, pg 426, lines 30-32. Schneier, therefore, discloses taking bits from the bit streams of events or functions, as well as *comparing phase jitter between clocks*, to obtain a random pool of bits. However, Schneier does *not* disclose capturing bits from a free-running timer as recited in claims 1 and 19. *See*, Schneier, pg 426, lines 6-37. As such, Schneier does not anticipate claims 1 and 19.

Therefore, claims 1 and 19 are not anticipated under Section 102 by the Schneier reference, and Applicants request withdrawal of the rejection of claims 1 and 19. Additionally, Applicants request withdrawal of the rejection of all claims dependent from claims 1 and 19, specifically claims 3-7, 20 and 22-26.

Claims 13-18 and 27-32

Applicants respectfully assert that the Utz reference does not anticipate independent claims 13 and 27 because it fails to disclose every element of the claimed invention. Specifically, claim 13 as amended recites "writing one or more bits to the seed pool upon termination of the first type of triggering event, the one or more bits of

data altering the signature value of the seed pool." Additionally, claim 27 as amended

recites security logic configured to "write one or more bits to the seed pool upon

termination of a first type of triggering event."

The Applicants assert the Examiner incorrectly alleges that the Utz reference

discloses "writing one or more bits to the seed pool upon termination of the first type

of triggering event, the one or more bits of data altering the signature value of the seed

pool (col. 6 lines 37-61)." Office Action, pg 5, lines 17-19. In sharp contrast to the

present application, the Utz reference never writes bits to a seed pool as the Examiner

alleges. The Utz reference discloses storing bits in nonvolatile memory 201 that are

used as a "start value." Col. 5, lines 34-38. The start value is loaded serially into the

11 bit RS/PRNG and the 13 bit RS/PRNG. *See*, Col. 5, lines 34-38; and Col. 6, lines

25-29. The start value, however, is *fixed.* Col 8, lines 58-64. Indeed, it is critical to

the proper operation of the apparatus disclosed in the Utz reference that the start value

never changes because it is used as an identifying value for a receiver to recognize a

transmitting remote device. *See*, col. 6, line 65 to col. 7 line 18. Furthermore, to

prevent changes in the start values, the non-volatile memory is made one-time

programmable by a programming disable fuse. Col. 8, line 65 to Col 9, line 4.

Therefore, not only does the UTZ reference never disclose the writing of bits to a seed

pool, the Utz reference makes it impossible to do so. As such, the Utz reference fails

to anticipate claims 13 and 27 under Section 102.

For at least the above stated reasons, Applicants respectfully request the withdrawal of the rejection of claims 13 and 27 and further request the withdrawal of the rejection of all claims depending therefrom, specifically, claims 14-18 and 29-32.

Rejections under 35 U.S.C. § 103

In the Office Action, the Examiner rejected claims 8-11 under 35 U.S.C. § 103(a) as being unpatentable over the Schneier reference as applied to claims 1-6, and further in view of Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone's "Handbook of Applied Cryptography", hereinafter referred to as "the Menezes reference." Applicants respectfully traverse this rejection.
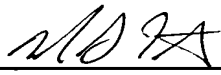
Applicants respectfully submit that claims 8-11 are allowable based on their dependency from claim 1 because the Menezes reference does not cure the deficiencies described above in regard to the Schneier reference. For this reason, claims 8-11 are believed to be allowable over the cited references taken alone or in combination with each other. Thus, Applicants respectfully request the withdrawal of the rejection of claims 8-11.

Conclusion

Applicants respectfully submit that all pending claims should be in condition

for allowance. However, if the Examiner wishes to resolve any other issues by way of

a telephone conference, the Examiner is kindly invited to contact the undersigned

attorney at the telephone number indicated below.

Respectfully submitted,

Date: September 22, 2005

Michael G. Fletcher
Reg. No. 32,777
(281) 970-4545

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400